APPENDIX B

SPECIAL CONSIDERATIONS FOR SAFEGUARDING PERSONAL INFORMATION DURING WORD PROCESSING

(See subsection D.2. of Chapter 1)

A. INTRODUCTION

1. Normally, word processing support is provided under two general concepts. They are:

a. Word processing centers (wPCs), and

b. Work groups or clusters.

2. A WPC generally provides support to one or more functional areas. Characteristically, the customer delivers (by written draft or dictation) the information to be processed to the WPC. The WPC processes the information and returns it to the customer. There are generally two types of WPCS.

a. A WPC may operate independent of the customer's function, providing service in much the same manner as a data processing installation provides ADP support, or a message center provides electronic message service, or

b. A WPC may work within a customer's function providing support to that function. The support being centralized in a WPC to take advantage of increased productivity.

3. A work group or cluster generally consists of one or more pieces of word processing equipment that are integrated into the functional office support system. The overall word processing and functional management may be one and the same. Depending on the size of the support job, there may be a work group or cluster manager. Normally, however, they will be located within or in close proximity to the functional area supported. Information flows in and out of the work group or cluster by normal office routine and the personnel are an integral part of the office staff.

B. MINIMUM STANDARDS OF PROTECTION

1. Regardless of configuration (WPC or work group), all personal data processed using word processing equipment shall be afforded the standards of protection required by subsection D.2. of Chapter 1.

2. The remaining special considerations discussed in this Appendix are primarily for WPCS operating independent of the customer's function. However, managers of other WPCs, work groups, and work clusters are encouraged to consider and adopt, when appropriate, the special considerations discussed herein.

3. WPCS that are not independent of a customer's function, work groups, and work clusters are not required to prepare formal written risk assessments (see section H., below).

C. WPC INFORMATION FLOW

1. In analyzing procedures required to safeguard adequately personal information in a WPC, the basic elements of WPC information flow and control must be considered. These are:

a. Information receipt.

b. Information processing.

c. Information return.

d. Information storage or filing.

2. WPCS do not control information acquisition or its ultimate use by the customers and, therefore, these are not addressed.

D. SAFEGUARDING INFORMATION DURING RECEIPT

1. The word processing manager shall establish procedures

a. That require each customer who requests that information subject to this Regulation be processed to identify specifically that information to the WPC personnel. This may be done by:

(1) Providing a check-off type entry on the WPC work requests;

(2) Requiring that the WPC work requests be stamped with a special legend, or that a special notation be made on the work requests;

(3) Predesignating specifically a class of documents as coming within the provisions of this Regulation (such as, all officer effectiveness reports, all recall rosters, and all ❑edical protocols).

(4) Using a special cover sheet both to alert the WPC personnel as to the type information, and to protect the document during transmittal;

(5) Requiring an oral warning on all dictation; or

(6) Any other procedures that ensure the WPC personnel are alerted to the fact that personal data subject to this Regulation is to be processed.

b. To ensure that the operators or other WPC personnel receiving data for processing that has not been identified to be under the provisions of this Regulation but that appear to be personal promptly call the information to the attention of the WPC supervisor or the customer;

c. To ensure that any request for the processing of personal data that the customer has not identified as being in a system of records and that appears to meet the criteria set forth in subsection Al. of Chapter 1 is called to the attention of the appropriate supervisory personnel and system manager.

2. The WPC supervisor shall ensure that personal information is not inadvertently compromised within the WPC.

E. SAFEGUARDING INFORMATION DURING PROCESSING

1. Each WPC supervisor shall establish internal safeguards that shall protect personal data from compromise while it is being processed.

2. Physical safeguards may include:

a. Controls on individual access to the center;

b. Machine configurations that reduce external access to the information being processed, or arrangements that alert the operator to the presence of others;

c. Using certain specific machines to process personal data;

d. Any other physical safeguards, to include special technical arrangements that will protect the data during processing.

3. Other safeguards may include:

a. Using only certain selected operators to process personal data;

b. Processing personal data only at certain times during the day without the WPC manager's specific authorization;

c. Using only certain tapes or diskettes to process and store personal data;

d. Using continuous tapes for dictation of personal data;

e. Requiring all WPC copies of documents to be marked specifically so as to prevent inadvertent compromise;

f. Returning extra copies and mistakes to the customer with the product;

g. Disposing of waste containing personal data in a special manner;

h. Any other local procedures that provide adequate protection to the data being processed.

F. SAFEGUARDING INFORMATION DURING RETURN

1. The WPC shall protect the data until it is returned to the customer or placed into a formal distribution channel.

2. In conjunction with the appropriate administrative support personnel and the WPC customers, the WPC manager shall establish procedures that protect the information from the time word processing is completed until it is returned to the customer.

3. Safeguarding procedures may include:

a. Releasing products only to specifically identified individuals;

b. Using sealed envelopes to transmit products to the customer;

c. Using special cover sheets to protect products similar to the one discussed in subparagraph D.1.a.(4), above;

d. Handcarrying products to the customers;

e. Using special messengers to return the products;

f. Any other procedures that protect adequately products from compromise while they are awaiting return or being returned to the customer.

G. SAFEGUARDS DURING STORAGE

1. The WPC manager shall ensure that all personal data retained in the center for any purpose (including samples) are protected properly.

2. Safeguarding procedures may include:

a. Marking all hard copies retained with special legends or designators;

b". Storing media containing personal data in separate files or areas;

c. Marking the storage containers for media containing personal data with special legends or notations;

d. Restricting the reuse of media used to process personal data or erasing automatically the media before reuse;

e. Establishing special criteria for the WPC retention of media used to store and process personal data;

f. Returning the media to the customer for retention with the file copies of the finished products;

g. Discouraging, when practical, the long-term storage of personal data in any form within the WPC;

h. Any other filing or storage procedures that safeguard adequately any personal information retained or filed within the WPC.

H. RISK ASSESSMENT FOR WPCs

1. Each WPC manager shall ensure that a formal, written risk assessment is prepared for each WPC that processes personal information subject to this Regulation.

2. The assessment shall address the areas discussed in sections D., E., F., and G. of this Appendix, as well as any special risks that the WPC location, configuration, or organization may present to the compromise or alteration of personal data being processed or stored.

3. A risk assessment shall be conducted at least every 5 years or whenever there is a change of equipment, equipment configuration, WPC location, WPC configuration or modification of the WPC facilities that either increases or decreases the likelihood of compromise of personal data.

4. Copies of the risk assessment shall be retained by the WPC manager and made available to appropriate inspectors , as well as to personnel studying equipment for facility upgrading or modification.

5. Every new WPC shall have a formal risk assessment completed before beginning the processing of personal data.

I. SPECIAL CONSIDERATIONS IN WPC DESIGN AND MODIFICATION

Procedures shall be established to ensure that all personnel involved in the design of WPCS or the acquisition of word processing equipment are aware of the special considerations required when processing personal data subject to this Regulation.